UNITED STATES PATENT APPLICATION

FOR

STEGANOGRAPHIC TECHNIQUES FOR SECURELY DELIVERING ELECTRONIC DIGITAL RIGHTS MANAGEMENT CONTROL INFORMATION OVER INSECURE COMMUNICATION CHANNELS

BY

DAVID M. VAN WIE

AND

ROBERT P. WEBER

STEGANOGRAPHIC TECHNIQUES FOR SECURELY DELIVERING ELECTRONIC DIGITAL RIGHTS MANAGEMENT CONTROL INFORMATION OVER INSECURE COMMUNICATION CHANNELS

CROSS REFERENCE TO RELATED APPLICATION

This application is related to commonly assigned copending application Serial Number 08/388,107 of Ginter et al., filed 13 February 1995, entitled "SYSTEMS AND METHODS FOR SECURE TRANSACTION MANAGEMENT AND ELECTRONIC RIGHTS PROTECTION" (attorney reference number 895-13). We incorporate by reference, into this application, the entire disclosure of this prior-filed Ginter et al. patent application just as if its entire written specification and drawings were expressly set forth in this application.

FIELD OF THE INVENTION

The present inventions relate generally to computer security, and more particularly to steganographic techniques for hiding or encoding electronic control information within an information signal carried by an insecure communications channel. Still more particularly, the present inventions relate to systems, methods and techniques that substantially invisibly and/or indelibly convey, over analog or other insecure communications channels, digital rights

management control information for use within a virtual distribution environment electronic rights management system.

BACKGROUND AND SUMMARY OF THE INVENTION

The world is becoming digital. Digital signals are everywhere – in our computers, television sets, VCRs, home stereos, and CD players. Digital processing – which operates on information "bits" (numerical "on" or "off" values) -- provides a degree of precision and protection from noise that cannot be matched by the older, "analog" formats we have used since the beginning of the electronic age.

Despite the clear advantage of digital communications, the older "analog" domain remains significant. Many of our most important information delivery mechanisms continue to be based on analog -- not digital -- signaling. In fact, most of our electronic entertainment, news, sports and music program material comes to us in the form of analog signals. For example:

- Television remains largely analog. Although the distribution of television programming to local cable systems is increasingly digital and most modern television sets include digital signal processing circuits, the local cable television "head end" continues to send television signals to the subscriber's set top box and television in analog – not digital -- form. It will cost a great deal to convert local cable distribution from analog to digital. In

the United States, for example, the widespread conversion from analog to digital television is projected to take no less than 15 years and perhaps even longer.

- In radio broadcasting, too, analog communication continues to reign supreme. Thousands of radio stations broadcast music, news and other programs every day in analog form. Except for a few experimental digital systems, practically all radio broadcasting is carried over analog communications channels.

- The movies and videos we rent at the local video tape rental store are analog.

- Commercially available music tape cassettes are recorded in analog formats.

Moreover, the "real world" is analog. Everything digital must ultimately be turned into something analog if we are to experience it; and conversely, everything analog must be turned into something digital if the power of modern digital technology will be used to handle it. Modern digital technology also allows people to get better quality for less money.

Despite the pervasiveness of analog signals, existing methods for managing rights and protecting copyright in the analog realm are primitive or non-existent. For example:

- Quality degradation inherent in multigenerational analog copying has not prevented a multi-billion dollar pirating industry from flourishing.

- Some methods for video tape copy and pay per view protection attempt to prevent any copying at all of commercially released content, or allow only one generation of copying. These methods can generally be easily circumvented.

- Not all existing devices respond appropriately to copy protection signals.

- Existing schemes are limited for example to "copy/no copy" controls.

- Copy protection for sound recordings has not been commercially implemented.

A related problem relates to the conversion of information between the analog and digital domains. Even if information is effectively protected and controlled initially using strong digital rights management techniques, an analog copy of the same information may no longer be securely protected.

For example, it is generally possible for someone to make an analog recording of program material initially delivered in digital

form. Some analog recordings based on digital originals are of quite good quality. For example, a Digital Versatile Disk ("DVD") player may convert a movie from digital to analog format and provide the analog signal to a high quality analog home VCR. The home VCR records the analog signal. A consumer now has a high quality analog copy of the original digital property. A person could re-record the analog signal on a DVD-R (a Digital Versatile Disk appliance and media supporting both read and write operations). This recording will in many circumstances have substantial quality – and would no longer be subject to "pay per view" or other digital rights management controls associated with the digital form of the same content.

Since analog formats will be with us for a long time to come, rightsholders such as film studios, video rental and distribution companies, music studios and distributors, and other value chain participants would very much like to have significantly better rights management capabilities for analog film, video, sound recordings and other content. Solving this problem generally requires a way to securely associate rights management information with the content being protected.

People have for many years been using various techniques allowing digital information to, in effect, ride "piggyback" on analog information signals. For example, since the 1960s, it has been common to digitally encode text information such as subtitles into

otherwise unused portions of analog television signals (e.g., within the so-called "Vertical Blanking Interval").

Unfortunately, sending digital information using such known digital encoding techniques is problematic because the digital information is not persistent. It is relatively easy to strip out or eliminate digital information encoded using prior techniques commonly employed for superimposing digital signals onto an analog information signal. Analog communications channels may commonly be subjected to various signal processing that may (intentionally or unintentionally) strip out digital information added to the analog signal – defeating any downstream system, process or technique that depends on the presence and readability of the digital information. For example, the television vertical blanking signal -- along with any signal components disposed within the vertical blanking interval -- is typically routinely eliminated whenever a video signal is processed by a computer.

Attempting to use insecure techniques for providing rights management is at best ineffective, and can be worse than no rights management at all. Unscrupulous people can strip out insecure control information altogether so that the corresponding information signal is subject to no controls at all – for example, defeating copy protection mechanisms and allowing users to avoid paying for rights usage. More nefariously, an unscrupulous person could alter an insecure system by substituting false control information in place of

the proper information. Such substitutions could, for example, divert payments to someone other than legitimate rights holders – facilitating electronic fraud and theft.

Prior, insecure techniques fail to solve the overall problem of how to provide and securely manage advanced automatic electronic rights management for analog and other information signals conveyed over an insecure communications channel. The lack of strong rights management for analog signals creates a huge gap in any comprehensive electronic rights management strategy, and makes it possible for consumers and others to circumvent – to at least some extent – even the strongest digital rights management technologies. Consequently, there is a real need to seamlessly integrate analog delivery models with modern electronic digital rights management techniques.

The present inventions solve these and other problems by providing "end to end" secure rights management protection allowing content providers and rights holders to be sure their content will be adequately protected -- irrespective of the types of devices, signaling formats and nature of signal processing within the content distribution chain. This "end to end" protection also allows authorized analog appliances to be easily, seamlessly and cost-effectively integrated into a modern digital rights management architecture.

The present inventions may provide a Virtual Distribution Environment ("VDE") in which electronic rights management control information may be delivered over insecure (e.g., analog) communications channels. This Virtual Distribution Environment is highly flexible and convenient, accommodating existing and new business models while also providing an unprecedented degree of flexibility in facilitating ad hoc creation of new arrangements and relationships between electronic commerce and value chain participants -- regardless of whether content is distributed in digital and/or analog formats.

The present inventions additionally provide the following important and advantageous features:

- An indelible and invisible, secure technique for providing rights management information.

- An indelible method of associating electronic commerce and/or rights management controls with analog content such as film, video, and sound recordings.

- Persistent association of the commerce and/or rights management controls with content from one end of a distribution system to the other -- regardless of the number and types of transformations between signaling

formats (for example, analog to digital, and digital to analog).

- The ability to specify "no copy/ one copy/ many copies" rights management rules, and also more complex rights and transaction pricing models (such as, for example, "pay per view" and others).

- The ability to fully and seamlessly integrate with comprehensive, general electronic rights management solutions (such as those disclosed in the Ginter et al. patent specification referenced above).

- Secure control information delivery in conjunction with authorized analog and other non-digital and/or non-secure information signal delivery mechanisms.

- The ability to provide more complex and/or more flexible commerce and/or rights management rules as content moves from the analog to the digital realm and back.

- The flexible ability to communicate commerce and/or rights management rules implementing new, updated, or additional business models to authorized analog and/or digital devices.

Briefly, the present inventions use "steganography" to substantially indelibly and substantially invisibly encode rights management and/or electronic commerce rules and controls within an information signal such as, for example, an analog signal or a digitized (for example, sampled) version of an analog signal.

The Greek term "steganography" refers to various "hidden writing" secret communication techniques that allow important messages to be securely carried over insecure communications channels. Here are some examples of steganography:

- In ancient Persia an important message was once tattooed on a trusted messenger's shaved scalp. The messenger then allowed his hair to grow back – completely hiding the message. Once the messenger made his way to his destination, he shaved his hair off again – exposing the secret message so the recipient could read it on the messenger's shaved scalp. See Kahn, David, The Codebreakers page 81 et seq. and page 513 et seq. (Macmillan 1967). This unusual technique for hiding a message is one illustration of "steganography."

- Another "steganographic" technique encodes a secret message within another, routine message. For example, the message "Hey Elmer, Lisa Parked My Edsel" encodes the secret message "HELP ME" -- the first letter of each word

of the message forming the letters of the secret message ("Hey Elmer, Lisa Parked My Edsel"). Variations on this technique can provide additional security, but the basic concept is the same – finding a way to hide a secret message within information that can or will be sent over an insecure channel.

- Invisible ink is another commonly used "steganography" technique. The secret message is written using a special disappearing or invisible ink. The message can be written on a blank piece of paper, or more commonly, on the back or front of the piece of paper carrying a routine-looking or legitimate letter or other written communication. The recipient performs a special process on the received document (e.g., exposing it to a chemical or other process that makes the invisible ink visible) so that he or she can read the message. Anyone intercepting the paper will be unable to detect the secret message – or even know that it is there – unless the interceptor knows to look for the invisible message and also knows how to treat the paper to make the invisible ink visible

The present inventions use steganography to ensure that encoded control information is both substantially invisible and substantially indelible as it passes over an insecure communications channel. At the receiving end, a secure, trusted component (such as a

protected processing environment described in Ginter et al.) recovers the steganographically-encoded control information, and uses the recovered information to perform electronic rights management (for example, on analog or other information signals carried over the same channel).

One specific aspect provided by the present inventions involve steganographically encoding digital rights management control information onto an information signal such as, for example, an analog or digitized television, video or radio signal. The steganographic encoding process substantially inextricably intertwines the digital control information with images, sounds and/or other content the information signal carries – but preferably without noticeably degrading or otherwise affecting those images, sounds and/or other content. It may be difficult to detect (even with educated signal processing techniques) that the analog signal has been steganographically encoded with a rights management control signal, and it may be difficult to eliminate the steganographically encoded control signal without destroying or degrading the other information or content the signal carries.

The present inventions also provide a secure, trusted protected processing environment to recover the steganographically-encoded control signal from the information signal, and to enforce rights management processes based on the recovered steganographically encoded control signal. This allows the information signal delivery

mechanism to be fully integrated (and made compatible) with a digital virtual distribution environment and/or other electronic rights management system.

In accordance with yet another aspect provided by this invention, steganographically encoded, digital rights management control information may be used in conjunction with a scrambled and/or encrypted information signal. The scrambling and/or encryption can be used to enforce the rights management provided in accordance with the steganographically encoded rights management control information. For example, the control signal can be steganographically decoded and used to control, at least in part, under what circumstances and/or how the information signal is to be descrambled and/or decrypted.

In accordance with yet another feature provided by the invention, digital certificates can be used to securely enforce steganographically encoded rights management control information.

In accordance with still another feature provided by the invention, steganography is used to encode an information signal with rights management control information in the form of one or more protected organizational structures having association with electronic controls. The electronic controls may, for example, define permitted and/or required operation(s) on content, and consequences of performing and/or failing to perform such operations. The

organizational structure(s) may identify, implicitly or explicitly, the content the electronic controls apply to. The organizational structure(s) may also define the extent of the content, and semantics of the content.

The type, amount and characteristics of the steganographically encoded rights management control information are flexible and programmable – providing a rich, diverse mechanism for accommodating a wide variety of rights management schemes. The control information can be used to securely enforce straightforward secure rights management consequences such as "copy/no copy/one copy" type controls -- but are by no means limited to such models. To the contrary, the present invention can be used to enable and enforce much richer, more complex rights management models – including for example those involving usage auditing, automatic electronic payment, and the use of additional electronic network connections. Moreover, the rights management control arrangements provided by the present invention are infinitely extensible and scaleable – fully accommodating future models as they are commercially deployed while preserving full compatibility with different (and possibly more limited) rights management models deployed during earlier stages.

The organizational structure(s) may be steganographically encoded in such a way that they are protected for purposes of secrecy and/or integrity. The employed steganographic techniques may

provide some degree of secrecy protection – or other security techniques (e.g., digital encryption, digital seals, etc.) may be used to provide a desired or requisite degree of security and/or integrity protection for the steganographically encoded information.

In one example, the organizational structure(s) may comprise digital electronic containers that securely contain corresponding digital electronic control information. Such containers may, for example, use cryptographic techniques. In other examples, the organizational structure(s) may define associations with other electronic control information. The other electronic control information may be delivered independently over the same or different communications path used to deliver the organizational structure(s).

In one example, the steganographic techniques employed may involve applying the organizational structure information in the form of high frequency "noise" to an analog information signal. Spectral transforms may be used to apply and recover such steganographically-encoded high frequency "noise." Since the high frequency noise components of the information signal may be essentially random, adding a pseudo-random steganographically encoded control signal component may introduce substantially no discernible information signal degradation, and may be difficult to strip out once introduced (at least without additional knowledge of how the signal was incorporated, which may include a shared secret).

In accordance with another aspect provided by the invention, a steganographic encoding process analyzes an information signal to determine how much excess bandwidth is available for steganographic encoding. The steganographic encoding process may use variable data rate encoding to apply more control information to parts of an information signal that use much less than all of the available communications channel bandwidth, and to apply less control information to parts of an information signal that use nearly all of the available communications channel bandwidth.

In accordance with still another aspect provided by the invention, multiple organizational structures may be steganographically encoded within a given information signal. The multiple organizational structures may apply to different corresponding portions of the information signal, and/or the multiple organizational structures may be repetitions or copies of one another to ensure that an electronic appliance has "late entry" and/or error correcting capability and/or can rapidly locate a pertinent organizational structure(s) starting from any arbitrary portion of the information signal stream.

In accordance with yet another aspect provided by this invention, an organizational structure may be steganographically encoded within a particular portion of a content-carrying information signal to which the organizational structure applies – thereby establishing an implicit correspondence between the organizational

structure and the identification and/or extent and/or semantics of the information content to which the organizational structure applies. The correspondence may, for example, include explicit components (e.g., internally stated start/end points), with the storage or other physical association determined by convenience (i.e., it may make sense to put the organizational structure close to where it is used, in order to avoid seeking around storage media to find it).

In accordance with yet another aspect provided by this invention, pointers can be steganographically encoded into parts of an information signal stream that has little excess available bandwidth. Such pointers may be used, for example, to direct an electronic appliance to portions of the information signal stream having more available bandwidth for steganographic encoding. Such pointers may provide improved steganographic decode access time – especially, for example, in applications in which the information signal stream is stored or otherwise available on a random access basis.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features and advantages provided by this invention may be better and more completely understood by referring to the following detailed description of presently preferred example embodiments in conjunction with the drawings, of which:

Figure 1 shows a virtual distribution environment providing steganographic encoding of digital rights management control information;

Figures 1A-1E show example electronic appliances embodying aspects of this invention;

Figure 2 shows an example of how electronic control information can be steganographically encoded within an image;

Figure 3 shows an example rights management component providing a steganographic decoding function;

Figure 4 shows an example of how steganographically encoded electronic control signals can be extracted and used for digital rights management;

Figures 5A-5D show example techniques for enforcing steganographically encoded rights management control information;

Figures 5E-5F show example "end to end" protected distribution systems provided in accordance with the invention;

Figure 6 shows an example of multiple sets of digital rights management control information steganographically encoded onto different parts of the same information signal stream;

Figure 7A shows an example detailed steganographic encoding process;

Figure 7B shows an example detailed steganographic decoding process;

Figure 8 shows an example frequency domain view of an example steganographic signal encoding technique;

Figure 9 shows an example use of a variable steganographic encoding rate to avoid exceeding channel bandwidths;

Figures 10 and 10A show how steganographically encoded pointers can be used to minimize access times to control signals steganographically encoded onto information signal streams available on a random access basis;

Figure 11 shows an example steganographically encoded organizational structure;

Figure 12 shows an example electronic appliance architecture having electronic rights management capabilities based at least in part on steganographically encoded control information;

Figures 13 and 13A show example control steps that may be performed by the Figure 12 appliance;

Figure 14 shows an example steganographic refresh arrangement; and

Figures 15A-15F show example distribution systems using steganographic encoding of rights management control information along at least one leg of an information distribution path.

DETAILED DESCRIPTION OF PRESENTLY PREFERRED EXAMPLE EMBODIMENTS

Figure 1 shows an example Virtual Distribution Environment (VDE) 50 employing steganography to deliver electronic digital rights management control information over an insecure (e.g., analog) communications channel.

In this example, a provider 60 delivers an information signal 70 to multiple electronic appliances 100(1), ..., 100(N). In this particular example, provider 60 is shown as being a television broadcaster that delivers an analog television information signal 70 over a wireless or cable communications path, and appliances 100(1), ..., 100(N) are shown as being home color television sets 106. As made clear by Figures 1A-1E, the present inventions may be used by a variety of different types of electronic appliances 100 receiving a variety of different types of information signals via a variety of different types of communications channels.

In the Figure 1 example, provider 60 steganographically encodes electronic rights management control information 126 into the information signal 70. This control information 126 is represented in this diagram as a traffic light because it may define permitted and/or required operation(s), and consequences of performing or failing to perform such operations. For example, control information 126 could specify that a viewer or class of viewers has permission to watch a particular program, is forbidden to watch a program, or may watch a program only under certain conditions (for example, based on paying a certain amount, being over a certain age, etc.). In this example the control information 126 is shown as being packaged within an electronic "container" 136. Container 136 (which in at least one example is provided by steganographic encoding techniques) is used to protect the integrity of the control information 126.

The provider 60 encodes the electronic rights management control information 126 onto information signal 70 using steganographic techniques that make the control information both:

- substantially invisible, and
- substantially indelible.

The control information 126 is substantially indelibly encoded because, in this example, it is substantially inextricably intertwined

with the television images and/or sound – and can't easily be eliminated from information signal 70 without destroying the images, sound or other information carried by the information signal. For example, steganographically encoding rights management control information will generally survive compression and decompression of a digitized analog signal, and will also survive repeated analog/digital/analog conversion sequences.

Even though the steganographically encoded control information 126 is substantially indelible, the television viewer is not bothered by the steganographically encoded information because the steganographically encoded rights management control information is, in this example, also encoded substantially invisibly. In fact, the viewer may not be able to see the steganographic control information at all -- and it may have no effect whatsoever on his or her viewing experience (other than in terms of the effect is has on associated rights management processes). The control information 126 is shown in dotted lines on the Figure 1 screens of television sets 106 to emphasize that the control information is substantially inextricably intertwined with the television images and/or sounds – and yet can't really be seen or noticed by the television viewer.

Figure 2 shows an example of how digital control information 126 may be encoded within an image 128 so that, in one particular example, it is both substantially invisible and substantially indelible. In this specific image context, for example, "substantially invisible"

may refer to the characteristic of the encoded control information as not substantially interfering with or adversely affecting the viewer's experience in viewing image 128 or otherwise using the content carried by the information signal 70 and/or that it is difficult to detect using various types of signal processing techniques, for example. For example, invisibility can be a measurable quantity (measured in a number of processor instructions, such as MIPS years, for example), and can be related to signal processing as opposed to the naked eye. In this context, "substantially indelible" can mean, for example, that the encoded digital control information is substantially inextricably intertwined with the content information, making it difficult for example to strip out the encoded digital control information without also damaging or degrading the content. Degree of indelibility may, for example, be measured by the number of processor instructions required to strip the information out.

Figure 2 shows that a slight rearrangement of picture element configuration in a small portion of image 128 is one way to steganographically encode electronic control information into the image to provide a substantially indelible, substantially invisible encoding. This encoding may be unnoticeable to the viewer, and yet it may be difficult to strip out or eliminate without also damaging the image. Steganographically encoding digital control information into the information signal 70 may effectively merge, from a practical standpoint, the digital control information with the other information carried by the signal (for example, television programming or other

content). The steganographic techniques make it difficult for someone to intentionally or unintentionally eliminate the encoded control information without damaging the content, but may (in one example) nevertheless hide the encoded control information so that it does not unduly detract from the content.

Since indelibility of the steganographic encoding provides persistence, indelibility may be more important than invisibility in at least some applications. For example, it may be desirable in some applications to use a shared secret to decode and then remove the steganographically encoded control information 126 before presenting the information signal (or its content) to the user. The steganographically encoded information need not be particularly invisible in this scenario. Even though someone with knowledge of the shared secret can remove the steganographically encoded information, it may nevertheless remain substantially indelible to anyone who doesn't know the shared secret required to remove it.

Organization Structures

Figure 1 shows that control information 126 may be packaged within one or more organizational structures such as secure digital containers 136. Containers 136 may be, for example, of the type described in the Ginter et al. patent specification in connection with Figures 17-26B. The organizational structure(s) may identify, implicitly or explicitly, the content the electronic controls apply to.

The organizational structure(s) may also define the extent of the content, and semantics of the content.

The organizational structure(s) may be encoded in such a way that they are protected for purposes of secrecy, authenticity and/or integrity. The employed steganographic technique may provide such protection, or another security technique may be used in conjunction with steganography to provide a desired or requisite degree of protection depending on the application. Containers 136 may, for example, use mathematical techniques called "encryption" that help guarantee the integrity and/or secrecy of the control information 126 they contain.

Example Rights Management Component

Each of the Figure 1 example appliances 100 may include a electronic digital rights management component 124. Rights management component 124 may, for example, comprise one or more tamper-resistant integrated circuit "chips". Components 124 may, for example, be of the general type described in detail at Figure 9 and following of the Ginter et al. patent specification. Briefly, Ginter et al. describes a Virtual Distribution Environment ("VDE") including multiple electronic appliances coupled together through a communications capability. Each electronic appliance has such a secure, tamper-resistant "protected processing environment" in which rights management processes may securely take place. The Virtual Distribution Environment delivers digital control information to the

protected processing environments by packaging the control information within secure electronic digital containers. This delivered control information provides at least part of the basis for performing electronic rights management functions within the protected processing environments.

The ability to securely deliver digital control information to such protected processing environments as embodied with components 124 is important at least because it increases flexibility and enhances functionality. For example, different digital control information can be delivered for the same or different electronic content. As one specific example, one set of rules may apply to a particular television program, another set of rules might apply to a particular film, and a still different set of rules could apply to a particular musical work. As yet another example, different classes of users of the same electronic content can receive different control information depending upon their respective needs.

Rights management components 124 are able to steganographically decode the control information 126 carried by the information signal 70. Components 124 use the decoded control information 126 to electronically manage rights. For example, components 126 may use the decoded control information 126 to control how the images and/or sound carried by information signal 70 may be used.

In one example, digital rights management component 124 may comprise or include one or more integrated circuit chips as shown in Figure 3. The Figure 3 example rights management component 124 includes an analog-to-digital converter 130, a steganographic decoder 132, and a rights management processor 134. Rights management processor 134 may include or comprise a protected processing environment 138 as described in Ginter et al. Figures 8-12, for example, providing a tamper-resistant execution environment for effecting the operations provided by electronic controls 126. Rights management component 124 may also include a steganographic encoder and a digital-to-analog converter (not shown).

The analog-to-digital converter (ADC) 130 shown in Figure 3 takes the incoming information signal 70 and – if it is in analog form -- converts it to a digital signal (see Figure 4, step "A"). Steganographic decoder 132 obtains the digital control information 126 from the resulting digital signal (Figure 4, step "B"). As mentioned above, digital control information 126 may define permitted and/or required operation(s) on the content carried by signal 70, and may further define consequences of performing and/or failing to perform such operations. Rights management processor 134 may manage these rights and/or permissions and associated consequences (Figure 4, step "C").

Example Electronic Appliances

The present inventions may be used with all sorts of different kinds of electronic appliances 100 each of which may include a rights management component 124. Figures 1A-1E show various example electronic appliances 100 embodying aspects of the present invention. For example:

- Figure 1A shows an example media player 102 capable of playing Digital Versatile Disks (DVDs) 104 on a home color television set 106. For example, media player 102 may provide analog output signals to television set 106, and may also process digitized video and/or audio analog signals stored on optical disk 104. Rights management component 124A provides digital rights protection based on steganographically encoded controls 126.

- Figure 1B shows an example set top box 108 that can receive cable television signals (for example, via a satellite dish antenna 110 from a satellite 112) for performance on home television set 106. Set top box 108 shown in Figure 1B may receive television signals from antenna 110 in analog scrambled or unscrambled form, and provide analog signals to television 106. Rights management component 124B provides digital rights protection based on steganographically encoded controls 126.

- Figure 1C shows an example radio receiver 114 that receives radio signals and plays the radio sound or music on a loud speaker 116. The radio receiver 114 of Figure 1C may receive analog radio signals, and provide analog audio signals to loud speaker 116. Rights management component 124C provides digital rights protection based on steganographically encoded controls 126.

- Figure 1D shows an example video cassette recorder 118 that can play back video and sound signals recorded on a video cassette tape 120 onto television 106. In Figure 1D, the video tape 120 may store video and audio signals in analog form, which VCR 118 may read and provide to television 106 in analog form. Rights management component 124D provides digital rights protection based on steganographically encoded controls 126.

- Figure 1E shows an example television camera that can capture video images and produce video signals for recording on a video cassette tape 120 and play back on television set 106. The Figure 1E camcorder 122 may generate analog video and audio signals for storage onto video tape 120, and/or may provide analog signals for processing by television 106. Rights management component 124E provides digital rights protection based on steganographically encoded controls 126.

Example Rights Management Enforcement Techniques

Different rights holders want different types of rights management and control. For example, some rights holders may be completely satisfied with a relatively simple "copy/no copy/one copy" rights management control model, whereas other rights holders may desire a richer, more complex rights management scheme. The present inventions flexibly accommodate a wide variety of electronic rights management techniques -- giving rightsholders extreme flexibility and programmability in defining, for example, commerce and rights management models that far exceed the simple "copy/no copy, one copy." Assuming a closed appliance, that is, one lacking at least an occasional connection to a payment method (e.g., Visa, MasterCard, American Express, electronic cash, Automated Clearinghouses (ACHs) and/or a Financial Clearinghouse that serves as the interface for at least one payment method), the following are non-limiting examples of steganographically encoded rights controls and associated consequences that can be accommodated by the present invention:

- Limiting use of a given property to a specified number of times this property can be used on a given appliance;
- Prohibiting digital to analog and analog to digital conversions;
- Ensuring that one analog or digital appliance will communicate the protected property only to another appliance that is also VDE enabled and capable of enforcing the controls associated with that property;

- Time-based rental models in which a consumer may "perform" or "play" the property an unlimited number of times in a given interval (assuming the appliance has a built-in secure time clock, can operatively connect itself to such a clock, or otherwise receive time from a reliable source);
- Enforcing an expiration date after which the property cannot be performed (also assuming access to a reliable time source);
- Associating different control sets with each of several properties on a single physical media. In one example, a "trailer" might have unlimited copying and use associated while a digital film property may have an associated control set that prevents any copying;
- Associating multiple control sets with a given property regardless of media and whether the appliance is closed or has an occasionally connected communications "backchannel."

An even more flexible and diverse array of rights controls and associated consequences are enabled by the present inventions if at least one appliance is connected to some form of communications "backchannel" between the appliance and some form of payment method. This backchannel may be a telephone call, the use of a modem, a computer data network, such as the Internet, a communications channel from a settop box to the head end or some

other point on a cable TV distribution system, or a hybrid arrangement involving high bandwidth distribution of analog properties with a slower return channel, a phone line and modem – just to name a few examples. Non-limiting examples of such more rights controls and associated consequences enabled by the present invention include the following:

- Associating with a given property in analog format new, independently delivered controls obtained from a rightsholder or other authorized source;
- A broad range of usage-based pricing models, including pay-per-view or pay-per-use;
- Creating permissions enabling excerpting of properties in analog formats, maintaining persistent control over those excerpts, and charging for those excerpts;
- Pay-per-use models in which a customer pays a specified price for each use of the property and/or different unit prices depending on the number of uses. In one example, the customer might pay $3.99 for the first viewing and $2.99 for each subsequent viewing; and,
- Controls that prevent an analog property being converted to digital format and then being transmitted or communicated except in a container with controls and/or with a pointer to a source of controls, that apply in a digital environment.

Figures 5A-5D show some examples of how rights management component 124 can enforce steganographically encoded digital rights management controls.

In the Figure 5A example, rights management component 124 controls an on/off switch 140 based on steganographically encoded electronic controls 126. Component 124 turns switch 140 on (for example, to allow the analog television signal to pass to television set 106) when electronic controls 126 permit, and otherwise opens (turns off) switch 140 to prevent the analog signal from reaching the output.

In a more secure example, the incoming analog signal is scrambled, and the Figure 5A on/off switch 140 is replaced by a Figure 5B descrambler 142 of conventional design. The descrambler 142 descrambles the analog input signal to provide a descrambled output under control of rights management component 124. Rights management component 124 allows descrambler 142 to descramble the analog signal only under conditions specified by electronic controls 126 that the component 124 obtains from the analog input signal. Scrambling the analog signal gives the rights management component 124 a relatively secure way of enforcing electronic controls 126 – since the rights management component can prevent the descrambler from operating unless conditions set by the controls are satisfied. The rights management function and the descrambling function may be integrated into a single component in which the descramble and decrypt functions of the rights management

component are essentially serving the same function, but may still be distinct to account for specialized approaches to descrambling that may not be sufficiently strong or interoperable with other environments to use generally. If they are separate components, the data path between them should be protected (for example, by ensuring that both components are in a tamper resistant enclosure, or using secure authentication and key exchange to send the descrambling sequence to the descrambler).

Figure 5C shows how digital certificates may be used to enforce steganographically encoded electronic controls 126. In this example, appliance 100A outputs content to another appliance 110D only if appliance 100D has a rights management component 124D that can enforce the electronic controls 126. In this example, there may be a "handshake" between the content supplying appliance 100A and the content receiving appliance 100D sufficient to ensure the content supplying appliance that the content receiving appliance will enforce the electronic controls 126. For example, the supplying appliance 100A's rights management component 124A may require the receiving appliance 100D's rights management component 124D to present a digital certificate 199 attesting to the fact that the receiving appliance 100D has a rights management component 124 fully capable of securely enforcing electronic controls 126. Receiving appliance 110D could present this digital certificate 199 by steganographically encoding it within an analog signal it provides to the supplying appliance over an analog signal channel for example

(the analog signal channel could be the same one the supplying appliance will use to deliver the steganographically encoded content). If a digital channel is available, the handshake can be over a digital link between the two appliances using, for example, secure authentication techniques disclosed in Ginter et al. and/or for example in Schneier, Applied Cryptography (2d Ed. Wiley 1996) at page 52 *et seq*.

Figure 5D shows that rights management component 124A can enforce electronic controls 126 by marking the content through "fingerprinting" and/or "watermarking" prior to releasing the content to a device that doesn't have a rights management component 124. See Ginter et al. patent specification, Figures 58A-58C. Such fingerprinting could involve using steganographic techniques to fingerprint the content. For example, a movie delivered using "conventional" containers as disclosed in Ginter et al. could use steganographically encoded containers "on the way" to the display device. Furthermore, it could include the identity of the user, etc. as well as the control information appropriate for the device. Another case could be text sent to a printer, using different steganographic encoding techniques such as line and/or character shifting.

End to End Protection

Figures 5E-5F illustrate how the persistent association with content provided by steganographically encoded electronic rights management control information 126 provides "end to end"

protection within an arbitrary information signal distribution system – irrespective of the processes the information signal is subjected to as it travels to its final destination.

Figure 5E shows an example of how the present inventions can be used to maintain end-to-end rights management protection over content initially distributed in an analog signal format. Figure 5F shows an example of how the present invention can be used to maintain end-to-end rights management protection over content initially distributed in digital form.

In the Figure 5E example, an analog signal transmission site (e.g., a radio or television broadcaster) transmits an analog signal A steganographically encoded with an organizational structure 136 including electronic controls 126. This analog signal A may be received by an electronic appliance 100A having a rights management component 124A as described above. Appliance 100A may, for example, convert the signal into digital and/or digitized format, and store the digitized version of the signal onto a digital storage medium 104. Electronic appliance 100A may play back the recorded digitized signal, convert the signal back to analog form, and deliver the analog signal A to a further electronic appliance 106B. In this example, electronic appliance 106B also has a rights management component 124B.

The steganographic techniques provided by the present invention ensure that the electronic controls 126 persist in the signal A delivered from appliance 100A to appliance 106B -- and from appliance 106B to still other appliances. Because of the substantial indelibility characteristics of the steganographically encoded control information 126, this information persists in the signal as stored on recording medium 104, in copies of the recorded signal produced by replaying the medium, and in further downstream versions of the signal.

This persistence will, for example, survive conversion from analog to digital format (e.g., sampling or "digitizing"), storage, and subsequent conversion from digital to analog format. For example, because the steganographically encoded control information 126 is substantially indelibly, substantially inextricably intertwined and integrated with the information signal A, the digitized version of the information signal that appliance 100A records on medium 104 will also contain the steganographically encoded control information 126. Similarly, when appliance 100A plays back the recording from medium 104, it will reproduce information signal A along with the steganographically encoded control information 126. The steganographically encoded control information 126 thus persists irrespective of digitization (or other processing) of signal A. In some cases, lossy compression techniques used on the data may remove high frequency noise -- thereby potentially damaging the steganographic channel. When these lossy compression techniques

are used or may be encountered, the steganographic encoding function should be matched to the compression algorithm(s) using conventional signal analysis techniques to avoid this consequence.

Similarly, appliance 106B may output further copies or versions of signal A in analog form and/or digital form. Because of its inherently persistent characteristics, the steganographically encoded control information 126 will be present in all subsequent versions of the signal outputted by appliance 106B – be they in analog format, digital format, or any other useful format.

Degrading a digital signal carrying control information is fatal – the rights management system typically may no longer function properly if even a single bit is altered. To avoid this, the preferred embodiment provides redundancy (repeating pointers and the organizational structures and/or any control information incorporated into the organizational structures), and also uses conventional error correction coding such as, for example, Reed-Solomon (or similar) error correcting codes. Additionally, because the steganographically encoded control information 126 is substantially inextricably intertwined with the desired content carried by information signal A, any process that degrades the steganographically encoded control information 126 will also tend to degrade the information signal's desired content. Although the steganographically encoded information may degrade (along with the content) in multi-generation "copies" of the signal, degraded copies may not be commercially

significant since the information content of the signal will be similarly degraded due to the substantially inextricable intertwining between the steganographically encoded control information 126 and the content carried by signal A. The refresh circuit shown in Figure 14 with appropriate error correcting capabilities is one way to prevent the steganographically encoded information from being degraded even if the rest of the information the signal carries becomes degraded.

The Figure 5F example shows content being initially distributed in digital form over a network to an electronic appliance 100J such as a personal computer. Personal computer 100J may convert the digitally delivered content to an analog signal A for distribution to other appliances 106B, 100A. Personal computer appliance 100J may include a rights management component 124J that ensures, based on controls 126, that appliance 100J does not release a version of the content associated with controls 126 that is not protected by the controls. In this example, rights management component 124J is capable of steganographically encoding the analog signal A with the control information 126 (e.g., it may perform the processes shown in Figure 7A below). Rights management component 124J enforces controls 126, at least in part, by ensuring that any analog version of the content associated with controls 126 is steganographically encoded with those controls. Further "downstream" appliances 106B, 100A may each include their

own rights management component 124 for use in interacting with steganographically encoded controls 126.

Example Control Information

Figure 6 shows that a particular information signal 70 may be encoded with many different containers 136 and associated rights management control sets 126. For example, different portions of an information signal 70 may be associated with different control information 126. In this example of a movie 270:

- a first "trailer" 272 may be associated with control information 126(1),
- a second trailer 274 may be associated with control information 126(2),
- a title section 276 may be associated with control information 126(3),
- the first five minutes of the movie may be associated with control information 126(4), and
- the rest of the movie may be associated with control information 126(5).

Control information portions 126(1), 126(2), 126(3), 126(4) and 126(5) may all be different. For example, control information 126(1) may permit the user to copy trailer 272, whereas control information 126(4) may prohibit the user from copying the first five minutes 278 of the film.

As shown in Figure 6, multiple, identical copies of control information 126(5) may be steganographically encoded onto the information signal 70. For example, control information 126(5) could be encoded once per minute onto the rest of movie 280. This redundancy allows a media player 102 or other electronic appliance 100 to rapidly obtain a copy of the control information 126(5) no matter where the user begins watching or playing the movie 270, and also helps ensure that transmission errors will not prevent the rights management component 124 from recovering at least one "good" copy of the organizational structure.

Example Steganographic Encoding and Decoding Processes

Figures 7A and 7B show example overall steganographic encoding and decoding processes, respectively. The Figure 7A process may be used to steganographically encode digital control information onto an analog signal, and Figure 7B performs the inverse operation of steganographically decoding the control information from the analog signal. Generally, the Figure 7A process may be performed at a supply point, and the Figure 7B process may be performed at a usage point. An electronic appliance 100 can be

both a supply point and a usage point, and so it may perform both the Figure 7A process and the Figure 7B process.

Referring to Figure 7A, the analog information signal 70 inputted to the steganographic encoding process may be any sort of information signal such as, for example, the analog signal shown in Graph A1. A conventional analog-to-digital conversion block 402 may be used, if necessary, to convert this analog input signal to a digitized signal (see Graph A2). A spectral transform block 404 may then be used to transform the digitized information from the time domain to the frequency domain. Spectral transform block 404 may be any conventional transformation such as, for example, a Fast Fourier Transform (FFT) or a Walsh Transform. An example of the resulting spectral information is shown in the A3 graph.

A steganographic encode block 406 may be used to steganographically encode digital control information 126, in clear text form and/or after encryption by a conventional digital encryption block 414 based on an encryption key Key_s. Steganographic information can be combined with a pseudo-random data stream (e.g. exclusive-or'd into the output of a DES engine) – in effect shuffling around the noise in the signal rather than replacing noise with the signal, *per se*. When protection is desired, the values in the pseudo-random stream can be protected by encryption (e.g. the key that initializes the DES engine should be protected). When the steganographic channel is "public" (e.g., unencrypted), the stream

should be readily reproducible (e.g. by using one of a preset collection of values shared by every device). A small portion (a "public header" -- see Ginter et al.) is always detectable using a shared preset value (that does not need to be protected, distinguishing it from the private header keys), may be provided to ensure that the rights management technology can be activated properly. Since the rights management component 124 at the receiving side needs to know how to descramble the signal, there normally will be an indication in the "public header" that names a key that will be used to unlock the private header (and so on, as described, for example, in Ginter et al.). Some publicly available, agreed upon preset values may be used to extract the "public header" information from the steganographically encoded channel.

Steganographic encode block 406 may be any conventional steganographic encoding arrangement capable of steganographically encoding a digital signal onto information signal 70. Steganographic encode step 406 may be based on a key K_c – allowing the same basic steganographic encoding and decoding transformations to be used by a wide variety of different appliances while still maintaining individuality and secrecy through the use of different steganographic keys.

In one example, the steganographic encoding step 406 may introduce the (encrypted) digital control information into the high frequency spectrum portion of the spectrally transformed information

signal 70. The spectrally transformed signal with steganographic encoding is shown in the Figure 7A Graph A4, and is shown in more detail in Figure 8. As Figure 8 shows, the steganographic encoding may affect the higher order frequency components of the spectrally transformed signal (see dotted perturbations in the fourth, fifth, sixth, seventh and eighth order components in Figure 8). The steganographic encoding may add to and/or subtract from the amplitudes of these higher order components. The effect of introducing high frequency steganographically encoded signal components may be to mask the steganographic encoding within the random high frequency noise inherently provided within information signal 70 – thereby providing substantial invisibility and substantial indelibility.

The amount of amplitude modification performed by steganographic encode step 406 may be limited in this example to ensure that the resulting steganographically encoded signal does not exceed the available channel bandwidth. See, for example,

- J. Millen, "Covert Channel Capacity," *IEEE Symposium on Security and Privacy* (1987).

- R. Browne, "An Entropy Conservation Law for Testing the Completeness of Covert Channel Analysis," *Fairfax 94*, pp 270 - 281 (1994).

- Moskovitz et al., "The Channel Capacity of a Certain Noisy Timing Channel,", *IEEE Trans. on Information Theory v IT-38 no. 4*, pp. 1330-43, (1992).

- Venkatraman, et al., "Capacity Estimation and Auditability of Network Covert Channels,", *Oakland 95*, pp. 186-298.

The following equations show the relationship between total bandwidth, bandwidth available for steganographic encoding, and the data rate of the steganographically encoded signal:

$$S = \int_{ta}^{tb} B(t)dt \qquad (1)$$

$$\equiv \sum_{i=a}^{b} B(i)\Delta t \qquad (1A)$$

where $\Delta t = t_{n+1} - t_n$, and
B is a function of time in bits/second.

In the above expressions, the function S corresponds to an area under a curve resulting from the product of B (bandwidth) and t (time). The parameter delta t refers to the "granularity" of the analog-to-digital conversion (i.e., 1/sampling rate).

Figure 9 shows an example plot of information signal bandwidth versus time. The total bandwidth available is limited by the bandwidth of the transmission channel – including the bandwidth of the storage medium (if any) used to deliver the signal, and the

bandwidth of the reproduction equipment. Since the total bandwidth depends on the inherent characteristics of the transmission channel used to communicate information signal 70, it is typically a fixed constant. Figure 9 shows that the bandwidth actually used by the information signal 70 typically varies with time. For example, although somewhat counterintuitive, the more complex an image, the more noise is typically available for "shuffling around" to create a steganographic channel. Of course, this isn't always true – a highly intricate geometric pattern may have very little noise available for encoding, and a simple picture of a cloud may have a great deal of noise available.

Steganographic encode block 406 can use an encoding rate and characteristic that ensures the steganographically encoded signal bandwidth doesn't exceed the total bandwidth available in the communication channel. Typically, the amount of bandwidth available for steganographic encoding may be on the order of on the average of 0.1% of the total transmission channel bandwidth – but as mentioned above, this bandwidth available for steganographic encoding may be unequally distributed with respect to time within the information signal stream 70 and may depend on the content of the information signal.

In this example, steganographic encode block 406 analyzes the content (e.g., by performing statistical weighted averaging), and provides a responsive variable steganographic encoding rate. For

example, steganographic encoding block 406 can use a high data rate during example time periods "II" and "IV" in which the information signal 70 has characteristics that allow high steganographic rate encoding without the resulting signal exceeding the available overall channel bandwidth. Encoding block 406 can use a low data rate during time periods "I" and "III" in which the information signal 70 has characteristics that do not allow high data rate steganographic encoding without exceeding available overall channel bandwidth. Steganographic encoding block 406 may use any number of different variable rates to accommodate different relationships between information signal 70 characteristics and available channel bandwidth.

Referring again to Figure 7A, the steganographically encoded spectral information outputted by steganographic encode block 406 may be subjected to an inverse spectral transform 408. Inverse spectral transform 408 in this example may perform the inverse of the transform performed by step 404 – outputting a version of the digitized time domain signal shown in Graph A2 but now bearing the steganographically encoded information (Graph A5). The digital control information steganographically encoded by block 406 may be substantially indelible and substantially invisible with respect to the Graph A5 signal – that is, it may be very difficult to eliminate the steganographically encoded information and it may also be very difficult to discern it.

This signal may be further scrambled and/or encrypted (e.g., based on a scrambling and/or encryption key Key_d) before being converted to analog form (shown in Graph A6) by a conventional digital-to-analog conversion block 412 (if necessary). Signal scrambling may be independent of steganographically encoded control information. For example, a good way to support existing devices is to not scramble the signal, and to use legislative means to ensure that each new device manufactured is equipped with rights management technology. Scrambling/encrypting of content, can be used to enforce use of rights management. If legislative means can enforce the use of rights management technology, encryption or scrambling of content may not be necessary (although a decision to provide cryptographic protection for the control information is independent of this factor and must be evaluated in light of protecting the rights management system). Rights holders can choose an enticement technique(s) based on their business model(s). The benefit of scrambling is that it provides technical means for enforcing rights management. The benefit of unscrambled content is support of hundreds of millions of devices in the installed base -- with the promise that new devices (potentially including computers) will enforce the control information even though they don't "have to" from a technical perspective.

The resulting steganographically encoded information signal 70 may then be transmitted over an insecure communications channel. Digital-to-analog conversion step 412 may be omitted if a

digital communications channel (e.g., an optical disk, a digital satellite link, etc.) is available to deliver the signal.

Figure 7B shows an example inverse process for recovering digital control information 126 from the steganographically encoded information signal 70. In this recovery example, the steganographically encoded analog signal is converted to a digitized signal (if necessary) by an analog-to-digital conversion step 402' and decrypted/descrambled (if necessary) by a decryption/descrambling block 422' to yield a facsimile of the inverse spectral transform block 408 output shown in Figure 7A. In this Figure 7B example, the analog-to-digital conversion block 402' is the inverse operation of Figure 7A, block 412, and the decrypt/descramble block 422' is the inverse of the Figure 7A scramble/encrypt block 410.

The resulting digitized signal provided by Figure 7B block 422' is spectrally transformed by step 404' (this may be the same spectral transform used in Figure 7A, block 404) to yield a steganographically encoded spectral signal A3. Steganographic decode block 424 may perform the inverse operation of the Figure 7A steganographic encode block 406 based on the same steganographic key Key_c (if a key-based steganographic encoding/decoding transformation is used). The output of steganographic decode block 424 may be decrypted by block 426 (the inverse of Figure 7A encrypt block 414 based on key Key_s) to provide recovered digital control information 126. The resulting

control information 126 may be used for performing electronic rights management functions Required keys may be delivered in containers and/or using the key distribution techniques and device initialization approaches disclosed in Ginter et al., for example.

Example Control Information Arrangements

In a further example shown in Figures 10 and 10A, steganographic encode block 406 may encode control information organizational structures such as secure containers (see Ginter et al., Figures 17-26B and associated text) during times when the content bandwidth is low relative to the total available bandwidth (see Figure 10 regions II and IV), and may not attempt to encode such organizational structures during times when the content bandwidth is high relative to the total available bandwidth (see Figure 10, regions I, III). In this way, steganographic encode block 406 may maximize the total bandwidth use without causing the steganographically encoded signal to exceed available bandwidth. As an optimization for certain applications, steganographic encode block 406 may encode "pointers" or other directional information into the information signal 70 during times when the content is such that it doesn't allow high data rate steganographic encoding of organizational structures 136. Multiple pointers and multiple "pointed to" locations can also help provide redundancy.

This particular Figure 10 example involving steganographic encoding of pointers 800 may be especially suited for content

delivery or presentation on random access storage media such as optical disks. Using such random access media, a content handling device may be able to rapidly "seek" to the place where an organizational structure is stored at a higher recorded bandwidth and then read the organizational structure at this higher bandwidth (See Figure 10A). For these example arrangements, steganographic encode block 406 in this example encodes, during periods when the content is such that it is not possible to steganographically encode organizational structures, pointers 800 that direct the content handling device to one or more places where the organizational structure appears in the content stream. In one example, pointers 800 might encode the location(s) on a storage medium (e.g., an optical disk 104 – see Figure 10A) at which the closest organizational structure is stored.

An optical disk player 102 with random access capability may "seek" to the place at which the closest organizational structure 136 is stored on the disk 104, and rapidly read the organizational structure off of the disk in less time than might be required to read an organizational structure that steganographic encode block 406 encodes at a lower data rate during times when the content bandwidth occupies most of the available channel bandwidth. In such arrangements, the process of reading a pointer 800, "seeking" to a position on the medium specified by the pointer, and then reading an organization structure 136 steganographically encoded at a high data rate may provide overall faster access times than if the organizational

structure was itself encoded at a lower data rate within the parts of the information signal stream used in this example to encode only pointers.

Figure 11 shows an example organizational structure 136 suitable for steganographic encoding similar to that shown in Figure 17 of the co-pending Ginter et al. application. In the case of container 136 with controls for an analog property, the organizational structure may include one or more permissions records 136d providing control sets 136e providing electronic controls especially for an analog device(s). The permissions record 136d may also provide a reference 136f at least one location or other external source for additional controls. This reference may be to an Internet "Uniform Resource Locator" (URL), for example. The organizational structure 136 may optionally include a content block 136g providing digital content subject to the controls. In this example, organizational structure 136 is encased in a protective "wrapper" 136x provided by the steganographic technique used to encode the organizational structure 136, digital encryption techniques, and/or a combination of the steganography and encryption. This protective wrapper 136x is used to ensure that the organizational structure 136 cannot be tampered with and maintains its integrity. Wrapper 136x may also provide a degree of confidentiality if required.

Detailed Example Electronic Appliance Architecture

Figure 12 shows an example detailed internal architecture for an example electronic appliance 100 such as optical disk player 102. In this specific example, rights management component 124 may be a tamper-resistant integrated circuit including internal microprocessor 200, flash memory 202 and cryptographic engine 204 (see Ginter et al. Figures 9-15B and associated text for a more detailed internal view of an example tamper-resistant rights management component 124 and a "protected processing environment" 138 it provides).

A main system bus 206 may couple rights management component 124 to a main system microprocessor 208 and various system components such as, for example, a CD-ROM decoder 210, a control and audio block 212, a video decoder 214, a digital output protection block 216, and a communications system 218. In this example, main microprocessor 208 controls the overall operations of appliance 100, with rights management component 124 performing security-related functions such as rights management and steganographic decoding.

In the Figure 12 example appliance 102, an optical pickup 220 reads information from optical disk 104 and provides it to RF amplifier 222. RF amplifier 222 provides its output to digital signal processor (DSP) 224, which processes the output in a conventional manner and also controls the orientation of the optical disk 104 relative to optical pickup 220 via a driver 226. DSP 224 coordinates

with a conventional CD-ROM decoder 210 to provide decoded digitized video and audio information. Decoder 210 operates in conjunction with a buffer memory 228, and may also cooperate with cryptographic engine 204 to ensure that any encrypted video information is decrypted appropriately.

The video output of CD-ROM decoder 210 may be decompressed by MPEG-2 video decoder 214 and applied via an NTSC and/or PAL encoder 230 to television 106. (In another example, the output could be in a non-interlaced format such as RGB rather than in interlaced formats such as NTSC and PAL.) Meanwhile, control and audio block 212 (which may operate in conjunction with its own buffer memory 232) may receive digitized audio information recorded on optical disk 204 via DSP 224 and CD-ROM decoder 210. Control and audio block 212 may provide this audio output to audio processing block 234 for output to loudspeakers 116. Control and audio block 212 may also provide an interface to the user via an infrared sensor 236 (for a remote control, for example), front-panel user controls 238 and/or an LED display 240.

In this example, security microprocessor 200 within rights management component 124 receives the digitized video and/or audio that DSP 224 reads from optical disk 104 via pickup 220 and RF amp 222. Security microprocessor 200 steganographically decodes this digitized analog information signal to recover the digital

control information 126 encoded onto the information signal. Security microprocessor 200 also performs rights management functions based on the digital control information 126 it recovers. In addition, if desired security microprocessor may remove the steganographic encoding from a received digitized analog signal (since it shares a secret such as the steganographic encoding key Key_s with the steganographic encoding point, it can remove the steganographic encoding) and/or steganographically encode a signal with received, augmented and/or new rights management control information.

In this example, microprocessor 200 may selectively control cryptography engine 204 to decrypt encrypted content provided by optical disk 104 – thus enforcing the rights management activities provided in accordance with electronic controls 126. Security component 124 may also control digital output protection block 216 in accordance with rights management control information 126 – thus, selectively permitting digital appliance 100 to output content in digital form. Rights management component 124 may take other steps (e.g., watermarking and/or fingerprinting information before releasing it) to provide a degree of copy protection and/or quality degradation to prevent or discourage someone from creating an unlimited number of high quality copies of the content of optical disk 104. Rules contained in the control information can also govern how other parts of the system behave. For example, the control information could specify that no sound can be played unless the

content is paid for. Another property may specify that certain copy protection schemes should be turned on in the NTSC encoder. Still another might disable the digital outputs of the device altogether, or unless an additional fee is paid.

Rights management component 124 (protected processing environment 138) may, in this particular example, communicate over a network 144 (such as, for example, the Internet or other data communications path) with other rights management related entities, such as, for example, clearinghouses and repositories. This "back channel" allows rights management component 124 to, for example, report usage and payment information and/or to retrieve additional rights management control information 126 to augment or supplement the control information it steganographically decodes.

Example Control Steps

Figure 13 shows example control steps that may be performed by protected processing environment 138 (e.g., security microprocessor 200) to provide electronic digital rights protection. The Figure 13 read/play routine 300 begins with protected processing environment 138 applying rules 126 – in effect, setting the initial state in which rights management can occur (Figure 13, block 302). Protected processing environment 138 then reads the output of CD-ROM decoder 310 (Figure 13, block 304) and obtains steganographically encoded data from the output stream (Figure 13, block 306). If protected processing environment 138 encounters the

beginning of the control information organizational structure ("yes" exit to decision block 308), the protected processing environment performs an initialization step (Figure 13, block 310) to begin receiving new control information 126 and then returns to block 302 to again apply current control information (Figure 13, block 302). If, on the other hand, protected processing environment 138 encounters a continuation of an organizational structure ("yes" exit to decision block 312, Figure 13), the protected processing environment stores the organizational structure information it has received (Figure 13, block 314) and turns again to the apply rules step (Figure 13, block 302).

If protected processing environment 138 encounters a pointer ("yes" exit to decision block 318), then the protected processing environment determines whether it already has received the corresponding organizational structure pointed to by the received pointer (Figure 13, decision block 320). The protected processing environment 138 retrieves the organizational structure if it does not already have it (Figure 13, block 322) – for example, by controlling DSP 224 to seek to the corresponding location on optical disk 104 indicated by the pointer, and by reading the organizational structure from the disk beginning at that disk location (Figure 13, block 322).

If protected processing environment 138 has received no organizational structures or pointers ("no" exits to each of decision blocks 308, 312, 318), then the protected processing environment

may determine whether there is any bandwidth available to carry control information. For example, some types of content stored on optical disk 104 may take up substantially all available channel bandwidths so that no bandwidth remains for steganographic encoding. If there is no available bandwidth for steganographic encoding ("no" exit to decision block 324), then the protected processing environment 138 may return to the "apply rules" block 302 and repeat steps 304-324 to wait until bandwidth is available for steganographic encoding. On the other hand, if there is bandwidth available and still no steganographically encoded information has appeared ("yes" exit to decision block 324, Figure 13), protected processing environment 138 performs an error handling routine that processes the exception (Figure 13, block 326) and determines whether the exception is critical (decision block 328). In some cases, protected processing environment 138 will continue to allow the appliance 100 to process the content, finding the error to be non-critical ("no" exit to decision block 328). An example of this would be a timer that permits playing for a period of time. In other cases (e.g., if the error conditions indicate that optical disk 104 has been tampered with), protected processing environment 138 may halt processing and return an error condition ("yes" exit to decision block 328, bubble 329).

Figure 13A shows example steps that may be performed by the Figure 13 "apply rules" routine 302. In this example, protected processing environment 138 may determine if it has received a

complete organizational structure on which to base rights management for the rights being read from optical disk 104 (Figure 13A, decision block 330). If the protected processing environment 138 has not received a complete organizational structure ("no" exit to decision block 330), it may disable content processing until it receives a complete organizational structure (Figure 13A, block 332). If protected processing environment 138 has a complete organizational structure ("yes" exit to decision block 330), it determines whether it has the current organizational structure (decision block 334). If the current organizational structure is present ("yes" exit to decision block 334), the protected processing environment 138 then processes the current operation with respect to the control information embodied in the organizational structure (Figure 13A, block 336). If the protected processing environment 138 does not have the current organizational structure ("no" exit to decision block 334), it determines whether it has an organizational structure that has the same identification as the current organizational structure (Figure 13A, decision block 338). The protected processing environment 138 may use that matching organizational structure as a default ("yes" exit to decision block 338, block 340). Otherwise, protected processing environment 138 disables content operations until it receives a current organizational structure ("no" exit to decision block 338, block 342).

As mentioned above, protected processing environment 138 may also perform any or all of the Figure 7A steganographic

encoding steps, and may also or alternatively remove the steganographic encoding from a signal by using a shared secret to generate a steganographic encoding stream and then subtracting that stream from the signal. Such techniques may be useful, for example, to allow protected processing environment 138 to encode new control information or to change the encoded control information. For example, the steganographically encoded control information might provide a chain of handling and control that authorizes certain protected processing environments to change some elements and add new elements to the control information 126. Protected processing environment 138 could:

- steganographically decode the signal using shared secrets to obtain the control information;

- modify the control information to the extent authorized by the control information;

- remove the steganographic encoding from the signal based on the shared secret; and

- steganographically encode the signal with the modified control information.

Example Refresh Capability

Figure 14 shows another example electronic appliance arrangement including a "refresh" capability involving both steganographic decoding and steganographic encoding. In this example, electronic appliance 100 includes a steganographic decoding block 424 as described above plus an additional steganographic encoding block 406. The appliance 100 may obtain the digital control information from the content signal, and then may "refresh" the extracted information (e.g., using coding techniques, such as, for example, Reed-Solomon decoding based on Reed-Solomon codes applied to the signal by the steganographic encoding process) to correct errors and otherwise accurately recover the digital control information. The error-corrected digital control information outputted by refresh decoder 900 may be applied to a steganographic encoding circuit 406 which steganographically encodes the content signal with the refreshed control information.

The Figure 14 refresh operation could, for example, be performed on a selective basis based on the encoded digital control information itself. For example, the control information might authorize appliance 100 to redistribute the content signal only under certain conditions – one of which is to ensure that a refreshed steganographic encoding of the same (or modified) digital control information is provided within the redistributed content signal.

Examples

Figure 15A shows an example analog signal distribution arrangement 500 provided in accordance with this invention. Within arrangement 500, a steganographic encode block 400 encodes an analog information signal A with rights management control information 126 and associated organizational structure(s) 136. The steganographically encoded information signal A′ is distributed by various mechanisms to user electronic appliances 100. For example, the encoded signal A′ may be broadcast wirelessly over the air by a broadcaster 60A, distributed over a cable television network by a cable television head end 502, and/or distributed via a satellite communications network 504. Encoded signal A′ may, during the process of being distributed, be converted from analog to digital form and back again. For example, the satellite uplink 504A may digitize signal A′ before transmitting it to the satellite 504b, and the satellite downlink 504c may convert the signal back to analog before providing it to user appliances 100. As explained above, the steganographically encoded control information 126 persists within the signal A′ despite conversions between analog and digital formats.

In this example, an example set top box user appliance 108 may receive the distributed steganographically encoded analog signal A′. Set top box 108 may include a rights management component 124 as described above, and may perform rights management operations and/or processes in response to and based on steganographically encoded control information 126.

Set top box 108 in this example may output the steganographically encoded analog signal (or a facsimile of it) to additional user electronic appliances such as, for example, a television set 106, a digital optical recording device (e.g., DVD-R) 102, and/or a video tape recorder 118. Each of these additional appliances 106, 102, 118 may include a rights management component 124 that performs electronic rights management based on the steganographically encoded control information 126. Any recordings made by recording devices 102, 118 may also be steganographically encoded.

Figure 15B shows another example analog signal distribution arrangement 510. In this example, a radio broadcaster 60B broadcasts an analog radio signal A′ that is steganographically encoded with associated rights management control information 126 and associated organizational structure(s) 136. A wire network 512 such as a cable television system may similarly distribute the same or different steganographically encoded analog radio signal A′. Broadcaster 60B and/or network 512 may deliver the steganographically encoded radio signal A′ to a user receiving appliance 100C such as a FM radio receiver 114. In this example, radio receiver 114 has a rights management component 124 that processes and automatically manages rights based on steganographically encoded controls 126. In this example, radio receiver 114 may (if permitted by controls 126) output steganographically encoded analog signal A′ to additional appliances

such as, for example, a digital recorder 102 and/or an analog recorder 514. In this example, each of appliances 100A, 100B has a rights management component 124 that electronically manages rights based on the steganographically encoded controls 126. Because the steganographically encoded controls 126 persist, recording devices 102, 514 record the steganographically encoded controls 126 in any recordings they make of signal A'. In one non-limiting example, when rights control information is encoded in steganographic sound recordings that are broadcast via radio or some other method, an airplay audit service can sample stations in a given market and identify particular properties being broadcast from "object identifier" information contained in the steganographically encoded VDE container.

Figure 15C shows an example signal distribution arrangement 520 in which the steganographically encoded analog signal A' is initially distributed in the same manner as shown in Figure 15A, and is then converted by an electronic appliance 100G such as a personal computer, for example, into a digital signal D. In this example, appliance 100G includes a rights management component 124 that manages rights based on steganographically encoded controls 126. Appliance 100G may convert received analog signal A' into digital form for distribution to and processing by digital appliances such as a digital high definition television 106B, a digital optical disk recorder 102, and/or a digital tape recorder 118a. In one example, the steganographically encoded control information 126 persists within

the digitized signal D. In another example, appliance 100G removes the steganographic encoding from received analog signal A′ and outputs a digital signal D that is "clean" and free of steganographic encoding – but is otherwise protected so that it remains persistently associated with the now-digital control information 126 (which appliance 100G may distribute, for example, within secure electronic containers 136 and digital, encrypted form. In one specific example, appliance 100G may package the received, digitized content from analog signal A′ within the same digital electronic container 136 that also contains associated control information that appliance 100G steganographically decodes from analog signal A′. In another specific example, appliance 100G may distribute controls 126 independently of the digital signal D – but under circumstances in which the rights management components 124 within each of digital appliances 106B, 102 and 118A all securely associate the control information with the now-digital content.

Figure 15D shows a similar distribution arrangement 530 for analog radio or other audio signals. In this example, appliance 100G may include a digital radio receiver that receives analog radio signal A′ and converts it into a digital information signal for distribution to digital recorders 102, 514A. As discussed above, appliance 100G may distribute the digitized analog signal A′ with steganographic encoding to appliances 102, 514A – each of which includes a rights management component 124 that may recover the steganographically-encoded control information 126 and perform

rights management functions based thereon. In another particular example, appliance 100G may remove the steganographic encoding from the content before distributing it in digital form – and user other techniques (such as those described in the above-referenced Ginter et al. patent specification) to provide a secure association between the now-digital content and the digital control information 126.

Figure 15E shows yet another example distribution arrangement 540 in which digital appliances 102, 100G distribute information in digital form to a digital television 106B. For example, appliance 102 may provide digital video signals D to digital television 106B by playing them back form DVD 104. DVD player 102 may provide controls 126 within electronic digital containers 136 to digital television 106B. Digital television 106B may include a rights management component 124C that manages rights in the digital content based on digitally-provided control information 126. Similarly, computer 100G may receive digital content and associated control information 126 from a digital network 144, and provide digital video signals D and associated controls 126 to digital television 106B.

In this example, digital television 106B includes an analog output that may provide analog television signals to additional devices, such as, for example, an analog video cassette recorder 118. In this example, the rights management component 124C within digital television 106B may steganographically encode the analog

television signal A with controls 126 and associated organizational structure(s) 136 before releasing the analog signal to the outside world.

Figure 15F shows a further example arrangement 550 in which a digital appliance 100G such as a personal computer receives digital video signal D and converts it into various analog television signal formats (e.g., NTSC/PAL and/or RGB) for output to analog devices such as an analog VCR 118, an analog set top box 108 and/or an analog television set 106A. In this example, a rights management component 124G within digital appliance 100G steganographically encodes the received digital controls 126 onto the analog signal A', A" before releasing the analog signal to the additional appliances 118, 106A, 108.

While the invention has been described in connection with what is presently considered to be the most practical and preferred embodiment, it is to be understood that the invention is not to be limited to the disclosed embodiment, but on the contrary, is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims.